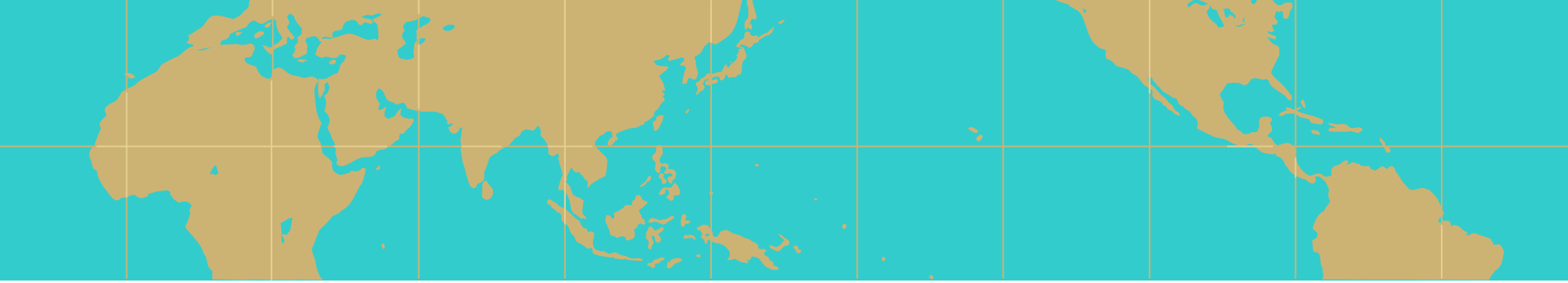


Introduction to System Safety

Steve Smith, Supervisor
System Safety Engineering Team
Federal Aviation Administration

Before We Start

- System Safety – Enhanced Safety Risk Management looking at all components – NOT individually, **but** as part of a bigger entity
- What it is and what is isn't!
  - Raising the bar on Safety (What it is)
  - Doesn't eliminate the need for Regulatory compliance (What it isn't)

System Safety Defined:

" The application of special technical and managerial skills to the systematic, ***forward-looking*** identification and control of hazards throughout the life cycle of a project, program, or activity..." *System Safety Engineering And Management.* (Roland & Moriarty).

Key Concepts

- ***Hazard*** -- A condition, event, or circumstance that could lead to or contribute to an unplanned or undesired event.
- ***Hazard identification*** -- Identification of a substance, activity, or condition as potentially posing a risk to human health or safety.
- ***Risk*** -- The expression of the impact of an undesired event in terms of severity and event likelihood.

What Is A System?

"An integrated composite of people, products, and processes that provide a capability to satisfy a stated need or objective."

Components of a System

- People
- Tools
- Procedures
- Materials
- Equipment
- Facilities
- Software
- Environment

Safety: More than the absence of accidents

- Safety is the goal of transforming the severity and likelihood of risk that is inherent in all human activity to lower, acceptable levels.
  .....*Patterns In Safety Thinking: A Literature Guide To Air Transportation Safety.* **(McIntyre).**

THE SYSTEM SAFETY VIEW

- Catastrophic Events Are Not Only the Result of Reliability Failures.
- Hazard Analysis Considers All Possible Catastrophic Events: Software, Human Error, Management and Latent Design Problems Impact Reliability Statistics.

➢ *A Statistical Probability Is Not a Hazard Control. A Reliability Number Is Only an Estimate. Not a Firm Promise.*

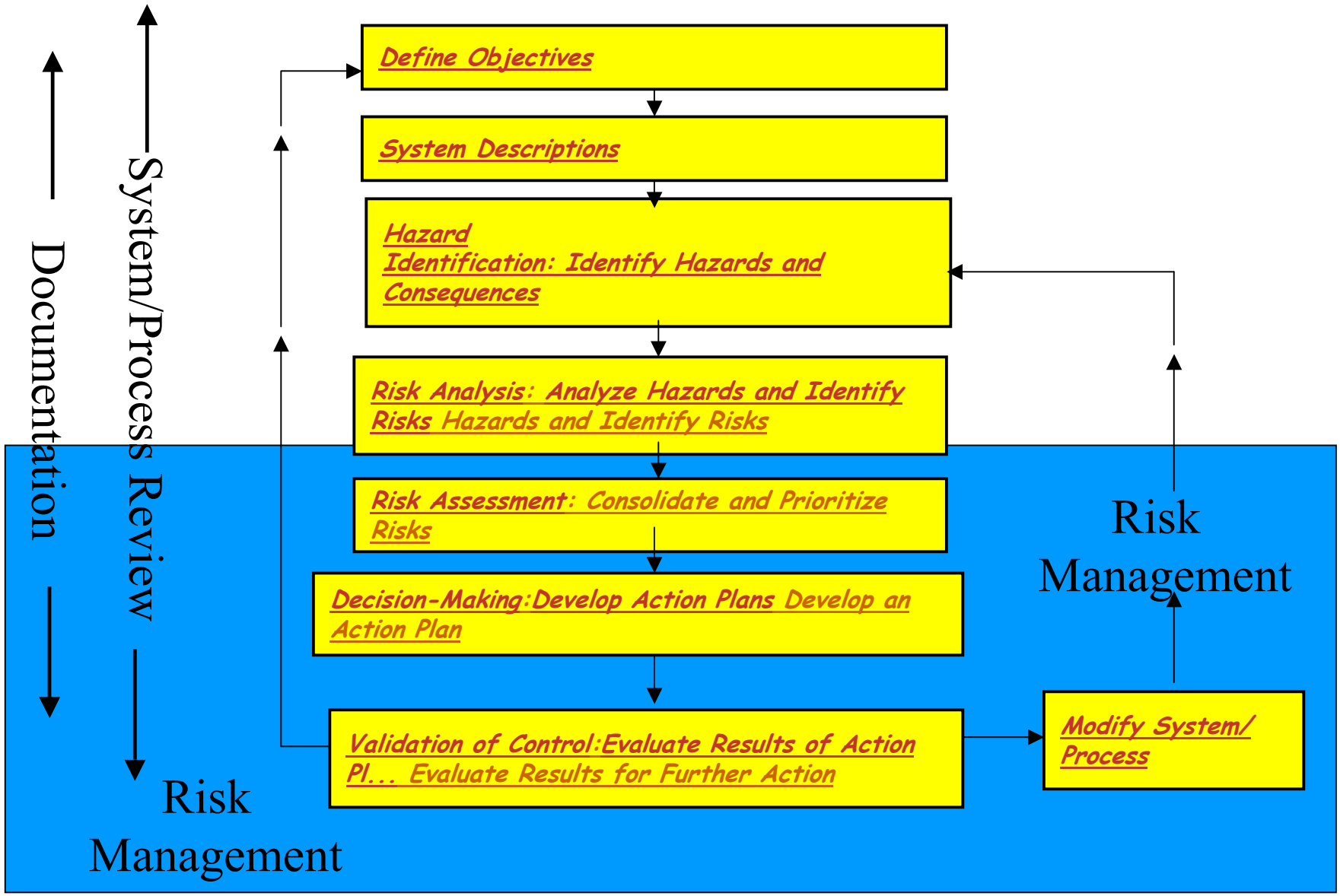
Understanding Risk. National Research Council

Draft FAA System Safety Handbook

Provides a Standardized Six Step Process

1. Plan
2. Hazard identification
3. Analysis
4. Assessment
5. Decision
6. Feedback

System Safety Process



1. Define Objectives

The first step in the System Safety process is to define the objectives of the system under review. These objectives are typically documented in business plans and operating specifications

2. System Description

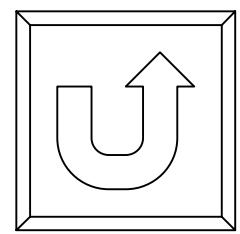
A description of the interactions among people, procedures, tools, materials, equipment, facilities, software, and the environment. This also includes descriptions of data available.

3. *Hazard Identification: Identify Hazards & Consequences*

Potential hazards may be identified from a number of internal and external sources. Generally, hazards are initially listed on a Preliminary Hazard List (PHL) then grouped by functional equivalence for analysis. Prior to risk analysis you must also include the consequence (undesired event) resulting from the hazard scenarios. Hazard scenarios may address the following: who, what where, when, why and how, regarding the hazard that is causing concern as well as its potential consequences. This provides an intermediate product that expresses the condition and the consequences that will be used during risk analysis.

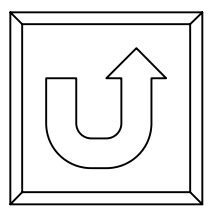
4. Risk Analysis: Analyze Hazards and Identify Risks

Risk analysis is the process whereby hazards are characterized for their likelihood and severity. Risk analysis looks at hazards to determine **what** can happen **when**. This can be either a qualitative or quantitative analysis. The inability to quantify and/or the lack of historical data on a particular hazard does not exclude the hazard from the need for analysis. Some type of Risk Assessment Matrix is normally used to determine the level of risk



5. Risk Assessment: Consolidate & Prioritize Risks

Risk Assessment is generally defined as the process of combining the impacts of risk elements discovered in risk analysis and comparing them against some acceptability criteria. Risk Assessment can include the consolidation of risks into risk sets that can be jointly mitigated. The results of this comparison are used in decision making.

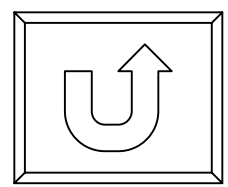


6. Decision Making: Develop Action Plans

This step begins with the receipt of a prioritized risk list. Review the list to determine how to address each risk, beginning with the highest prioritized risk. The four options that may be chosen for a risk are transfer, eliminate, accept, or mitigate (T.E.A.M). Generally, design engineering follows the "safety order of precedence": 1) Design for minimum risk, 2) Incorporate safety devices, 3) Provide warning devices, or 4) Develop procedures and training

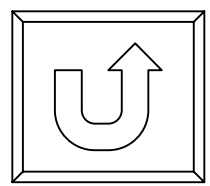
7. Validations and Control: Evaluate Results of Action Plan for Further Action

Validation and control begins with (1) the results of scheduled analyses on the effectiveness of actions taken (this will include identification of data to be collected and identification of triggering events if possible; then developing a plan to review the data collected) and (2) the current status of each prioritized risk. If the residual risk is acceptable, then documentation is required to reflect the modification to the system, and the rationale for accepting the risk. If it is unacceptable, an alternative action plan may be needed, or a modification to the system/process may be necessary.



8. Modify System/Process (If needed)

If the status of a risk should change or the mitigating action does not produce the intended effect, a determination must be made as to why. It may be that the wrong hazard was being addressed, or the system/process needs to be modified. In either case, one would then re-enter the system safety process at the hazard identification step.



Safety Risk Management – A part of System Safety

- Safety Risk Management - Does two things:
  - 1. Requires owner of a process (Both FAA and Whomever) to examine its process from a whole new perspective than we do today. Examine why something works, what happens when it doesn't, etc. as well as "What don't we want to occur."
  - 2. Fosters communication between and among the participants. No communication, less identification of risk and fewer effective mitigations!

System Safety Process Model

- System Safety's primary objective is to manage safety risk by identifying, assessing, and eliminating or controlling safety-related hazards, to acceptable risk levels.
- System Safety and risk management complement traditional, time-honored and valuable regulatory oversight and surveillance methods. Anticipating and controlling hazards by designing them out of the system is the key to System Safety.

System Safety for Accident Prevention

- The fundamental premise of the discipline of System Safety is accident prevention.
- Risk Management methods help attain that goal.
- Simply identifying hazards and reporting instances of non-compliance *after* a specific problem has occurred is essentially looking backward.

Does data play a role?